UNITED STATES PATENT AND TRADEMARK OFFICE.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,412	06/29/2000	Howard C. Herbert	042390.P7704	7770

7590 06/08/2004

William W Schaal
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/607,412	HERBERT ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36 and 38-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 15-42* is/are rejected.

7)☒ Claim(s) *12-14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *See Continuation Sheet*.

Continuation of Attachment(s) 6). Other: Japanese Translation of Cited Reference.

Detailed Office Action

Claims 1-36 and 38-41 have been fully reconsidered and are pending. Claims 1, 17, 27, 30, 33, 39 and 41 have been amended. Claim 37 has been canceled.

The examiner has included a copy of the written English translation of the entire Yamazaki reference for Applicant's convenience.

Response to Amendment

The amendment to claim 27 has warranted the withdrawal of the previous 35 USC 112 rejection.

Response to Arguments

Applicant's arguments with respect to claims 1-11, and 15-36 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments see page 9, filed 4-26-04, with respect to claim 12 have been fully considered and are persuasive. The rejection of claim 12-14 has been

withdrawn. Claims 12-14 are however objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicant's arguments filed 4-26-04 with respect to claim 38 have been fully considered but they are not persuasive. Claim 38 has been amended to include the limitations of canceled claim 37. Claim 38 does not include the new limitations that was added to independent claims 1, 17, and 33. As such, the previous rejection of claims 37 and 38 now apply to amended claim 38 because no new scope is defined. Claim 38 already included the limitation that the destinations were physically separate. Giving the broadest reasonable interpretation of physically separate, the examiner has determined this limitation is taught and suggested by Yamazaki. Yamazaki teaches sending the parts of keys through different channels. Receiving a part of a key on a CD-ROM in the mail is a physically different destination than receiving another part of the key through the Internet.

Claim Rejections - 35 USC ' 103

Claims 1-11, 15-36, 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki et al in view of Schneier (Applied Cryptography).

As per claim 1, Yamazaki et al teach:

storing a current sort encryption key (SEK) at a first destination in an internal memory of an electronic component (see paragraph [0006]);

storing a next SEK at the first destination in the internal memory [0006];

providing the electronic component to a second destination [0005]; and

recovering a private key at the second destination from a key bundle based on the current SEK, the next SEK and a plurality of bundles received at the second destination [0008].

Yamazaki et al are silent in expressly disclosing that each key bundle includes a key identifier and an integrity check. Schneier teaches sending a key with a key identifier and an integrity check to allow a more secure key exchange (bottom of pg. 55, SKID protocol). This key bundle would compliment the other confidential information that is sent in another channel of communication as a means to verify and correctly associate one part of key information with the corresponding parts. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Yamazaki because it would allow for a more secure key distribution protocol.

As per claim 17, Yamazaki et al teach a method comprising:

at a first destination, recovering a current sort encryption key (SEK) and a next SEK based on information within a first plurality of incoming bundles [0024] and

storing the current SEK and the next SEK in an internal memory of an electronic component [0025], [0051]; and

at a second destination, upon receipt of the electronic component,

recovering a private key from a key bundle based on the current SEK, the next SEK and a second plurality of incoming bundles [0059].

Yamazaki et al are silent in expressly disclosing that each key bundle includes a key identifier and an integrity check. Schneier teaches sending a key with a key identifier and an integrity check to allow a more secure key exchange (bottom of pg. 55, SKID protocol). This key bundle would compliment the other confidential information that is sent in another channel of communication as a means to verify and correctly associate one part of key information with the corresponding parts. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Yamazaki because it would allow for a more secure key distribution protocol.

As per claim 2, transferring at least a first bundle to the first destination via a first link [0007]; and

transferring at least a second bundle to the first destination via a first out of-band information carrying mechanism [0007].

As per claims 3 and 21, Yamazaki et al teach the first bundle includes a plurality of configuration window (CWIN) bundles [0005].

As per claims 4 and 22, Yamazaki et al teach each of the CWIN bundles includes a configuration window material, the configuration window includes

(i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated with the next SEK, (iv) the next SEK and (v) a group integrity check value for a first encryption key and a second encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claims 5 and 23, Yamazaki et al teach wherein the configuration window material

is encrypted with the first encryption key and the second encryption key [0008].

As per claims 6 and 24, Yamazaki et al teach each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key [0006].

As per claims 7 and 25, Yamazaki et al teach the second bundle includes a plurality of sort encryption key (SEK) bundles [0060].

As per claims 8 and 26, Yamazaki et al teach each of the SEK bundles includes

(i) a sort encryption key, (ii) a key identifier associated with the sort encryption key and (iii) an integrity check value associated with the sort encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claim 9, Yamazaki et al teach transferring the plurality of bundles to the second destination, the plurality of bundles includes a third bundle and a fourth bundle [0060].

As per claims 27, Yamazaki et al teach the second plurality of bundles includes a plurality of first part bundle encryption key (BEKp2) bundles and a plurality of second part bundle encryption key (BEKP2) bundles [0008].

As per claim 28, Yamazaki et al teach each of the BEKp2 bundles includes a second part of the bundle encryption key and a group integrity check value for a first encryption key and a second encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claims 29, Yamazaki et al teach one of the BEKp2 bundles includes a first part of the bundle encryption key and an integrity check value associated with the current SEK [0022].

As per claim 30, Yamazaki et al teach one of the BEKp2 bundles includes a first part of the bundle encryption key and an integrity check value associated with the next SEK [0022].

As per claim 31, Yamazaki et al teach the bundle encryption key is recovered upon recovering the first and second parts of the bundle encryption key [0051].

As per claim 32, Yamazaki et al teach the private key is recovered using the bundle encryption key [0051].

As per claim 33, Yamazaki et al teach a method comprising:

receiving at least a first bundle via a first link [0007];

receiving at least a second bundle via a first out-of-band information carrying mechanism [0007];

recovering a current sort encryption key (SEK) and a next SEK based on information contained in the first bundle and the second bundle [0051]; and

storing the current SEK and the next SEK in an internal memory of an electronic component [0022].

Yamazaki et al are silent in expressly disclosing that each key bundle includes a key identifier and an integrity check. Schneier teaches sending a key with a key identifier and an integrity check to allow a more secure key exchange (bottom of pg. 55, SKID protocol). This key bundle would compliment the other confidential information that is

sent in another channel of communication as a means to verify and correctly associate one part of key information with the corresponding parts. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Yamazaki because it would allow for a more secure key distribution protocol.

As per claim 34, Yamazaki et al teach transferring the electronic component to a second destination [0005].

As per claims 10, 11, and 35, Yamazaki et al are silent in expressly the third bundle is transferred to the second destination via a second link, and that the fourth bundle is transferred to the second destination via a second out-of-band information carrying medium. Yamazaki teaches that multiple bundles are transferred to the destination over at least to channels, one in band, and one out of band [0060]. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamazaki et al by having additional bundles exceeding the first two taught by Yamazaki et al, to also travel along the same communication channels.

As per claim 15, Yamazaki et al teach the fourth bundle includes a plurality of configuration encryption key (CEK) bundles [0005].

As per claim 16, Yamazaki et al teach each of the CEK bundles includes (i) a configuration encryption key, (ii) a key identifier associated with the configuration encryption key and (iii) an integrity check value associated with the configuration encryption key [0006], [0022-0025], [0041], [0057-0059].

As per claim 38, Yamazaki et al teach a source to output a first collection of encrypted keying material and a second collection of encrypted keying material [0006];

a first destination to receive the first collection of encrypted keying material, to decrypt keying material originating from the first collection of encrypted keying material for recovery of sort encryption keying material and to store the sort encryption keying material into an internal memory of an electronic component [0005]; and

a second destination to receive the second collection of encrypted keying material, to decrypt keying material originating from the second collection of encrypted keying material for recovery of at least private key for subsequent loading in the internal memory [0005-0008]. Yamazaki et al teach wherein the first destination is physically separated from the second destination [0006].

As per claim 39, Yamazaki et al teach wherein the sort encryption keying material includes a current sort encryption key (SEK) and a next SEK [0006].

As per claim 41, Yamazaki et al teach the second destination further recovers a digital certificate chain from the second collection of keying material and loads the digital certificate chain into the internal memory [0049].

As per claims 18-20 and 40, Yamazaki et al are silent in expressly disclosing that a period of validity is associated with the current SEK and that when the time of validity expires, the private key is not recovered. The use of a timestamps associated with a private key is taught by Schneier (pgs. 60-61). The timestamp prevents replay attacks by an intruder to gain unprivileged information. It would be advantageous to use a timestamp in a key exchange protocol. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Schneier within the system of Yamazaki et al because it would make the system more secure by reducing the chance of replay attacks by an intruder.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100